



UNITED STATES PATENT AND TRADEMARK OFFICE

SJ
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/924,990	08/08/2001	Huibert Den Boer	PHN 15,813B	5411
24737	7590	06/21/2005	EXAMINER	
PHILIPS INTELLECTUAL PROPERTY & STANDARDS			PARTHASARATHY, PRAMILA	
P.O. BOX 3001			ART UNIT	PAPER NUMBER
BRIARCLIFF MANOR, NY 10510			2136	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/924,990	DEN BOER, HUIBERT
	Examiner	Art Unit
	Pramila Parthasarathy	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 August 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 21-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 21-31, 34, 36 - 39 is/are rejected.
- 7) Claim(s) 32, 33 and 40 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. 08/859591.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date: _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |



DETAILED ACTION

1. This action is in response to communication filed on August 08, 2001.

Preliminary amendments to the claims were filed on August 08, 2001, with new Claims 21 – 40 and claims 1 – 20 were cancelled.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 21 – 40 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 – 10 of U.S. Patent No. 6,298,136. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the patent and in the instant case all elements of Claims 21 – 40 correspond to Claims 1 – 10 of U.S. Patent No. 6,298,136.

A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Bern, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

3. Although the conflicting claims are not identical, they are not patentably distinct from each other because the following list of claims in instant application are taught in the Patent 6,298,136:

Instant Claim	6,298,136 Claim
21 – 24, 26	1
25, 27	2
28, 29	3
31	4
32	5
33	6

34	7
35	8
36 – 39	9
40	10

More specifically,

4. Regarding Claim 21 as an exemplary in instant application:

This claim recites "...digital input block M with a first digital key K1 to produce a data block B1 which non-linearly depends on said selected part M1 and said first digital key k1" and "...said digital output block from said data block B1 and the remaining part of the digital input data block M, wherein said merging step is performed by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in a single step", which is recited in the Claim 1 of 6,298,136.

5. Regarding Claim 36 as an exemplary in instant application:

This claim recites "...a first input for obtaining said digital input block," "a second input for obtaining a first key K1;" and "a cryptographic processing portion arranged to convert the digital input block into the digital output block by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in one step and producing a data block B1 which non-linearly depends on said selected

part M1 and said first key K1, where a selected part of said digital output block is derived from said data block B1.", which is recited in the Claim 9 of 6,298,136.

6. Regarding Claim 30 in instant application:

This claim recites "... swapping the sub-blocks t1, and t_{2n-1-i} , for I=0 to n-1; and concatenating the swapped sub-blocks", which is not recited in 6,298,136. However, concatenation and swapping units are standard techniques to those skilled in the art. One would be obvious to modify the claim of 6,298,136 and use these techniques because these operations add confusion to the cipher making it more difficult to cryptanalysis.

7. The exemplary Claim 21 in instant application is generic to the species of invention covered by claim 1 of the patent 6,298,136. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior ad defeats any generic claim) 4 . This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982)., Schneller, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).

Claim Objections

8. Claim 40 is objected to because of the following informalities: Claim 40 recites, "A processor as claimed in claim 19, wherein ...". Claim 19 has now been cancelled. Examiner for the purpose of examination reads Claim 40 as "A processor as claimed in claim 39, wherein ...".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claim 30 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The new Claim 30 read, "... concatenating the swapped sub-blocks.".

With respect to "concatenating", although the specification discloses merging selected part of sub-blocks, the specification does not disclose a program segment

concatenating the swapped sub-blocks. The specification does not indicate how the sub-blocks are concatenated. Applicant's remarks (filled on 8/8/2001) do not clarify the program segment concatenating the swapped sub-blocks.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 23 – 35 and 38 – 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "substantially" in claims 23, 24, 27 and 38 is a relative term which renders the claim indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

For examining purposes, "substantially having equal length" is broadly interpreted as "having any length".

Dependent claims 25, 26, 28 – 35, 39 and 40 are rejected at least by the virtue of their dependency on the dependent claims.

11. Claims 36 – 40 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. Claim 36 recites "A processor for ...a first input for obtaining, a second input for obtaining ..., a cryptographic processing portion". The word(s) "input" and "processing" should have "means" in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no "means" is specified by the word(s) "input" or "processing" it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph.

For examining purposes, "input for obtaining" is broadly interpreted as "input means for obtaining" and "cryptographic processing portion" is broadly interpreted as "cryptographic processing means for processing".

13. Claim 37 recites "A processor for ...a third input for obtaining,". The word "input" should have "means" in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no "means" is specified by the word "input" it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph.

For examining purposes, "input for obtaining" is broadly interpreted as "input means for obtaining" and "cryptographic processing portion" is broadly interpreted as "cryptographic processing means for processing".

Dependent claims 37 – 40 are rejected at least by the virtue of their dependency on the dependent claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 21 – 40 are rejected under 35 U.S.C. 102(e) as being anticipated over Garcken et al. (U.S. Patent Number 5,778,074, hereafter “Garcken”).

15. Regarding Claim 21, Garcken discloses
a program portion for merging a selected part M1 of said digital input data block M with a first digital key K1 to produce a data block B1 which non-linearly depends on said selected part M1 and said first digital key K1 (Column 5 line 59 – Column 6 line 5); and
a program portion for deriving said digital output block from said data block B1 and the remaining part of the digital input data block M, wherein said merging step is performed by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in a single step (Column 5 line 59 – Column 6 line 16) .

16. Regarding Claim 36, Garcken discloses

a first input for obtaining said digital input block (Column 5 line 59 – Column 6 line 5);

a second input for obtaining a first key K1 (Column 5 line 59 – Column 6 line 26);;

and

a cryptographic processing portion arranged to convert the digital input block into the digital output block by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in one step and producing a data block B1 which non-linearly depends on said selected part M1 and said first key K1, where a selected part of said digital output block is derived from said data block B1 (Column 5 line 59 – Column 6 line 5).

17. Claims 22 – 25, 37 and 38 are rejected as applied above in rejecting claims 21 and 36. Furthermore, Garcken teaches converting digital input data block into output data blocks, dividing each block into sub block which is combined with a key and a second sub block into a combined data, both blocks through the same merging process using a second nonlinear merging (Column 6 lines 2 – 54).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 26 – 31, 34 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcken et al. (U.S. Patent Number 5,778,074, hereafter “Garcken”) in view of Koopman, Jr. (U.S. Patent Number 5,757,923, hereafter “Koopman”).

19. Claims 26 – 31, 34 and 39 are rejected as applied above in rejecting claims 21, 26, 36 and 38. Furthermore, Garcken discloses splits each block into a plurality of sub blocks and keys each using a different a different subkey and first sub divides one and then the other sub blocks applying multiplying multiple keying and conversion/merging to reassemble the cipher block (Column 6 line 2 – Column 7 line 13 and Column 10 lines32 – Column 11 line 25. Garcken does not disclose Galois field, however, Koopman discloses a Galois field GF(2^n) over which elements are derived (Column 2 line 51). One would be motivated to combine and use these techniques because these operations add diffusion and confusion to the cipher making it more difficult to cryptanalysis.

Claim Objections

20. Claims 32, 33 and 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

21. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific

disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
June 14, 2005.



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100